SECRET

AGENDA
Continuity and Contingency Planning

Monday, 2 November 1981
Room 2D-47

0900 - Welcome and Introductions
Working Group Chairman, [redacted] ODP 25X1

0915 - An Overview of Agency Emergency Planning
[redacted] Chief, Planning Staff, Office of Policy & Planning 25X1

1000 - Break

1015 - OC's IH Survivability Study, Recommendations and Issues
Study Chairman, [redacted] OC 25X1

1045 - ODP's Emergency Planning MFR Discussion
[redacted] ODP 25X1

1130 - Lunch

1300 - OL's Utility Support System; Nature, History, Problems and Plans
[redacted] Chief, Hqs Engineering Branch/RECD/OL 25X1

1400 - Discussion of the Overview Point Paper. Comment and Review. Response to Questions

1500 - Discussion of the Robustness Point Paper. Comment and Review. Response to Questions

1700 - Adjourn

Tuesday, 3 November 1981
Room 5G-00

0900 - Presentation on Communications Switching System Availability (A_o)
[redacted] OC/ED 25X1

0945 - Presentation on Data Processing System Availability (A_o)
[redacted] ODP/ED 25X1

1030 - Break

1045-onward - Discussion of Tentative Goals and Objectives. Instructions for Working Group.
Chairman, [redacted] 25X1

SECRET

REFERENCES

Copies of the following publications are available from the Chairman or IHSA representative.

1. OC - Information Handling Survivability Study, dated 3 September 1980

2. ODP - MFR on Emergency Planning, by [redacted] dated 28 October 1980 25X1

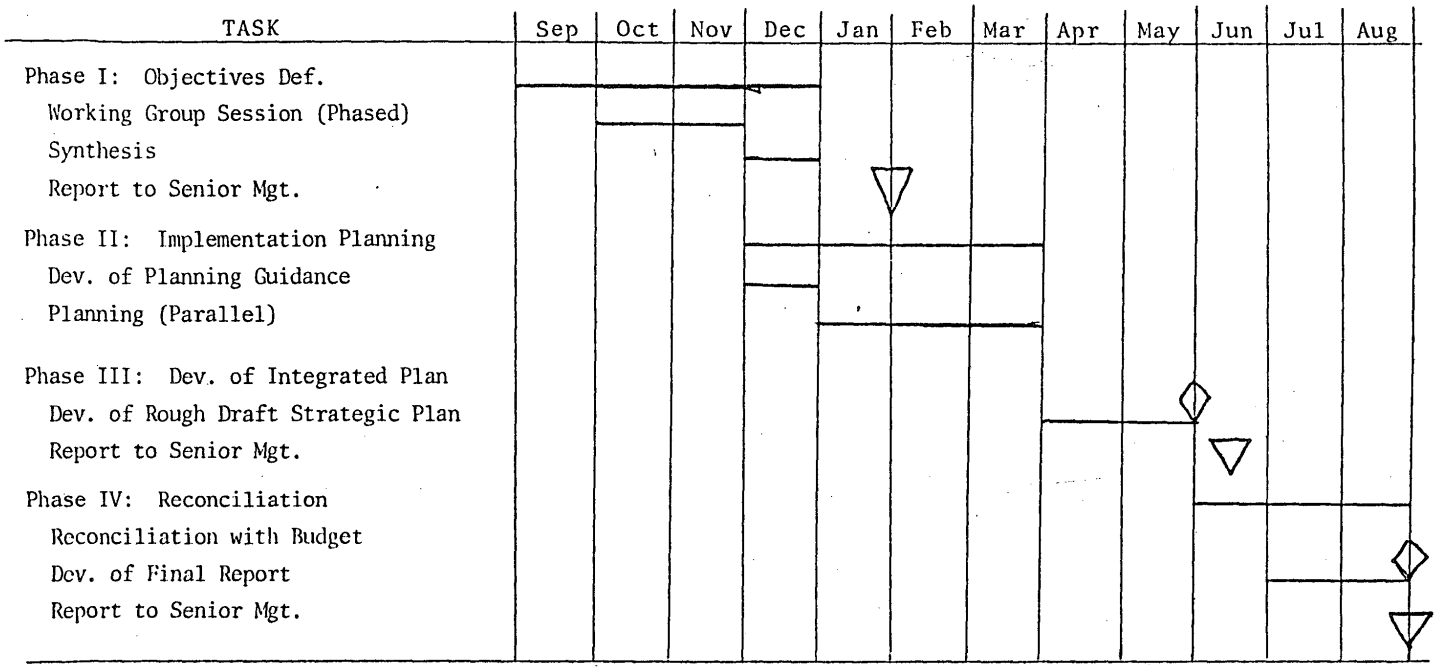
3. NBS - Federal Information Processing Standards (FIPS) Pub 87, Guidelines for ADP Contingency Planning, dated 27 March 1981

4. Processing System Availability Charts covering recent Fiscal Years

5. Communications Planning Issue (Recapitalization Paper), First Two Sections: Challenge and Staff Network, dated 17 August 1981

6. Information Handling Study-1980, Final Report of the Information Handling Task Force, dated 5 September 1980

PLAN FOR IHSs STRATEGIC PLAN



Legend

◇ Documentation

▽ Presentation

SECRET

WORKING PAPER

Continuity and Contingency Overview Paper

OUTLINE

1. Introduction

   a. Objective
   b. Definitions

2. Current Trends

   a. Political Considerations
   b. Recognition of Need
   c. Architectural Considerations

3. Current Planning Efforts

   a. [redacted] 25X1
   b. OC Initiatives
   c. ODP Initiatives
   d. OL Initiatives

4. Threat Assessments

5. Issues

   a. Affordability
   b. Interoperability
   c. Reserve Capacity

6. Discussion Questions

OVERVIEW PAPER

Continuity and Contingency

1. Introduction

a. Objective

The objective of this point paper is to focus attention on system continuity and contingency planning for Agency IHS services. Our intent is to examine the more vulnerable aspects of the Agency's information handling systems (IHSs) identifying critical functions and susceptible choke points, gain perspective from a users view of the criticality of these individual system weaknesses and generate user-backed input for the Agency's IHS Strategic Plan.

25X1

b. Definitions

Continuity is defined as the capability to sustain the intelligence process when the system is impacted by forces that cause a stressful condition. Contingency planning is those steps that are taken to secure continuity of operations under the circumstances mentioned above. Other terms which describe a system's ability to sustain failure or damage and continue to provide the services that users need include availability, serviceability, reliability and survivability. From a systems view, the term robustness describes these characteristics. It refers to the resilience and reliability of a system -- its ability to continue to function without failure, or given failure or damage, with minimum degradation of performance. In addition, robustness refers to the strength of the system in the sense of its ability to absorb any additional demands that may be placed upon it in a stressed mode.

2. Current Trends

a. Political Unrest

Events of recent past as well as press and intelligence reports have confirmed that the terrorist threat is ever-present and increasing in intensity and sophistication. The vulnerable position of many Agency domestic outstations to terrorist attack has been readily apparent for many years.

25X1

Next 6 Page(s) In Document Denied

SECRET

WORKING PAPER

Robustness

I. Background

The constrained budget environment of the past six or eight years and the government-wide zero based budgeting process have taken their toll on the Agency Information Handling Systems (IHS). We now have an environment that is near an optimum with respect to cost versus performance. Concomitantly, our systems are fragile. For the most part, it is a single thread environment. As a broad generalization, there are a large number of single points of failure in our IHSs; it is far too likely that any single failure will bring down a system, albeit perhaps, only briefly.

This lack of robustness of our systems will not be acceptable for our foreseeable future. The Agency has an ever increasing level of on-line, real-time operational responsibilities. Furthermore, it must provide continuity of operation during contingencies and war. The current robustness of our IHSs falls far short of serving these needs. It provides inadequate availability for the projected numbers of users of communications and data processing functionalities for the mid-80's, and inadequate survivability in the advent that hostile action or an accident disables a major functional entity.

The reason that the current situation exists, of course, is that robustness costs money and contributes little, if anything, to performance. To improve robustness, we have to invest in it, perhaps at the expense of providing other IHS functionalities. (Such a tradeoff will always obtain, because there will always be more things on our "wish" list than there are funds to implement them.) As a consequence, we have to be careful in specifying robustness objectives. It is tempting to specify lofty goals, but it should be recognized that accomplishment of these goals costs, in terms of other things not done. The problem is intensified because the cost of availability tends to rise exponentially as the level approaches 1.0.

Since there will be acute limitations of funds in the light of all the objectives the Agency has for new IHS functionalities, the governing philosophy should probably be for the Agency to work its way out of the fragility corner via the planned evolution of the architecture. As we develop new capabilities we should assure that they meet our robustness criteria and provide architectural redundancy with respect to current systems. We should not modify the existing systems simply to improve robustness--that is simply unaffordable.

While the robustness objectives of the IHS strategic plan need to be specific to be meaningful, it should be recognized that they are

not based on hard analyses. These will have to come later, and they will doubtless result in some modification of our goals. But by being specific at this point, it is possible to assure a common understanding and mutual agreement as to what we need to accomplish, relative to where we are today.

25X1

Next 22 Page(s) In Document Denied